The Crime of Speech

How Arab Governments Use the Law to Silence Expression Online

Wafa Ben Hassine

Table of Contents

I. Executive Summary

Since the revolts that took the region by storm in 2010 and 2011, the Arab world continues to face a diverse set of sociopolitical challenges. Each of the countries studied in this report–Egypt, Jordan, Saudi Arabia and Tunisia–has responded to the uprisings differently. Government reactions range from the expansion of rights, to social upheaval, to civil war. Additionally, the rise of the so-called Islamic State (ISIS) poses a threat to all four countries.

In reaction to fundamentalist groups often relying on the Internet for propaganda and recruiting, several governments in the Arab world have passed shortsighted cybercrime and counterterrorism laws–ostensibly to combat these groups on the digital front.[1] It is unclear what kind of motivation lies behind these laws; however, as it stands, national security appears to give lawmakers a convenient excuse to crack down on rights.

Research has found that each country's law enforcement uses a wide range of mechanisms to stifle dissent. These laws do little to prevent activity by terrorist groups such as ISIS. Instead, they frequently explicitly criminalize speech that the government finds threatening to its legitimacy, and are often used to supplement other totalitarian practices to target and stifle unwanted or politically critical speech.

In order to better understand how online speech in particular is targeted, this research tracked instances of arrest, detention, and imprisonment of individuals for speaking online under the pretenses of counterterrorism or fighting cybercrime. I tracked cases from 2011 to the present.

I have found that Saudi Arabia and Jordan rely on counterterrorism and cybercrime regulations to prosecute online activism. Egypt uses a new anti-protest law passed in 2014 and Tunisia, in contrast, relies on old defamation and anti-drug laws that have been used for decades prior to the revolution. In all four countries, the prosecution and imprisonment of Internet users for expressing themselves effectively chills critical speech and cripples civil discourse–all the while neglecting to create any long-term and comprehensive solution to the threat of terrorist movements.

This report hopes to raise awareness of the human rights abuses that are committed by these governments in the name of countering acts of terrorism. It also hopes to galvanize policy-makers to consider alternative measures that prioritize human rights and the rule of law as fundamental bases of the fight against terrorism.

1 "Tunisia's Ineffective Counterterrorism Law," Sarah Mersch, SADA, Carnegie Endowment for International Peace, 6 August 2015 http://carnegieendowment.org/sada/?fa=60958.

II. Introduction

As individuals concerned with rights in the Arab world, we often express concern over the possibility of law enforcement regimes abusing national security rhetoric to clamp down on fundamental rights.[2] However, researchers do not track which laws are used in furtherance of this rhetoric, nor do we have solid data on instances of arrest and time served in jails. In some cases, we lack even the most basic consistent terminology with which to discuss these laws across regions: for instance, the terms "cybercrime" and "cyber-terrorism" have very different meanings in the United States than in the Arab world. In the United States, the term "cybercrime" is used to describe a number of individual laws whose subject matter ranges from gaining unlawful access to protected network systems[3] to fraudulent identity theft and software piracy.[4] In some countries in the Arab world, laws on cybercrime and counterterrorism are actually laws against certain types of online speech. My research aims to demonstrate these differences in understanding and help track how varying interpretations are used to target rights defenders in the region.

This project has three main goals: (1) researching counterterrorism and cyber-security laws in the Arab world that limit various rights online and outlining the processes through which such laws are executed, and (2) analyzing effects on local human rights advocates, and (3) outlining incidents of local authorities abusing vague legislative language and subsequently targeting individuals. These three areas represent key data gaps for human rights activists as well as legislators who are focused on the expansion of digital rights.

The goal of this report is to provide those working in the field a better understanding of the diversity of mechanisms used in prosecuting free expression and thought in the Arab world. Most importantly, it aims to highlight the variety of laws and practices used by different governments in the region: the Arab world is far from monolithic, and the legal strategies used to stifle dissent differ both from the United States and from one another.

2 *See*, "Counter-Terror Law Endangers Rights," Article 19, where eight organizations express concern over .recently passed counterterrorism law in Tunisia. Organizations include Human Rights Watch, Amnesty International, Article 19, and the International Federation for Human Rights, 31 July 2015, https://www.article19.org/resources.php/resource/38072/en/tunisia:-counter-terror-law-endangers-rights

3 *See*, Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act, Pub. L. 107-56 (H.R. 3162), 115 Stat. 272, 107th Cong., 1st Sess. (Oct. 26, 2001), § 814, 816, https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf.

4 *See*, United States Federal Cybercrime Laws, https://digitalenterprise.org/governance/us_code.html.

Initial hypothesis

My initial hypothesis in starting this research was that Arab governments rely predominantly on cybercrime and counterterrorism laws to crack down on meaningful assembly and expression online.

Revised hypothesis

My revised hypothesis shifted significantly after researching and indexing cases of arrest, detention, and/or imprisonment in Egypt, Jordan, Saudi Arabia, and Tunisia. It became apparent that each country's respective law enforcement authorities used unique mechanisms to prosecute human rights defenders. While most governments did classify the action in question as "terrorism" or as an act that "threatens national security," only Jordan and Saudi Arabia showed consistency in prosecuting under counterterrorism laws. Tunisia relied on defamation laws, and Egypt on its anti-demonstration law. This is a lesson in and of itself: due to the diversity of legal and political contexts, the region is far from monolithic. Each country has its own legal methods for stifling expression.

Study limitations

It is difficult to create an exhaustive report of suppression of speech in the four countries we studied. Here are some limitations to this work.

Lack of available, reliable data

For all reported cases of arrest and or detention due to online activity, there will undoubtedly be others that are kept entirely in the dark. For this research, I have relied entirely on publicly accessible information; therefore, the report is sure to undercount the actual number of incidents. The figures presented in the report should be considered lower-bound estimates.

Access to data

Most limiting in this study was the lack of access to important documents such as court decisions, appeals, and debated draft legislation. I did my best in securing appropriate contacts for access to needed information.

Longitudinal effects in rapidly changing ecosystems

The Middle East and North Africa (MENA) region is experiencing unique and rapidly shifting regional circumstances. This is especially true in Tunisia, where the government is now reacting to "terrorist threats" with unprecedented and blanketed actions against human rights defenders. Egypt also represents a delicate ecosystem of political polarization that may change at any moment.

III. Methodology

The goal of this research project is to assess counterterrorism (CT) and cybercrime (CC) laws in select Arab countries and explore how these laws are used to target online activists.

Phases

I conducted the research in three phases.

Phase 1

Phase 1 of the research project involved three sub-steps.

Sub-phase 1.1

The first step in Phase 1 was conducting topical research on the socio-political happenings in every country in the Arab world and determining whether or not each respective country was fit for inclusion as a case study in this project. I created a set of questions for this purpose, as well as a simplified flowchart to guide the process. The flowchart is attached as an appendix.

Sub-phase 1.2

The second step was selecting the countries for study and compiling relevant legislation, orders or decrees, and government statements on counterterrorism and cybercrime policy. I have mainly relied on the Arab Digital Rights Dataset[5] created by Social Media Exchange (SMEX) to source these documents.

Sub-phase 1.3

The final part of Phase 1 studied the laws in question and exposed gaps that could lead to their abuse. This phase was essentially a quasi-legal policy-analysis.

Phase 2

Phase 2 established a database of instances of arrest and/or detention of end users under counterterrorism and cybercrime laws. In conducting this phase of research, I looked at news alerts, articles, and calls to action by non-governmental organizations in raising awareness of human rights violations.

5 Social Media Exchange, Arab Digital Rights Dataset, https://smex.silk.co/.

Phase 3

Phase 3 tracked the process in which the legislation had been executed and (when applicable and available) looked at the judiciary's response to the cases. For example: were most of the charges dropped against the accused? Did the judiciary seek to strike a balance between national security and online freedom? This largely depends on the environment and history of the country under study, and I will be providing background and context for each country.

Through the documentation and aggregation of these data-points, I used an evidence-based approach to expose trends and patterns in governments using counterterrorism and cybercrime laws as pretext for targeting human rights work done online.

Need to better track cases

There is an acute need to create a better mechanism for tracking instances of arrest and/or detention of online speech under the pretense of fighting terrorism. In creating the database, this research did most of the labor manually by going through various news sources and press releases from non-governmental organizations. For the purposes of this report, this proved very time-consuming. This process can be streamlined and improved: for example, nonprofits can start logging these instances into a shared database that is open to the public.

Definitions

Counterterrorism law

MENA governments often use the guise of fighting terrorism to control the pace of democratic development. As such, counterterrorism laws frequently fail to address real issues of security and instead regulate speech and curtail fundamental rights such as privacy, assembly, and expression. I have identified a counterterrorism law as any type of national document with legal force that explicitly purports to fight terrorism and the maintain the "integrity of the state" or "national security." These documents can take on the form of legislation, presidential/governmental decrees, or court decisions.

> "The terms 'cybercrime' and 'cyber-terrorism have very different meanings in the United States than in the Arab world."

Cybercrime law

Cybercrime laws are used in a similar way. I have identified a cybercrime law as any type of national document with legal force that explicitly purports to combat common digital threats such as fraud, online stalking, money laundering, and harassment. These documents can take on the form of legislation, presidential/governmental decrees, or court decisions.

Cyber-activists

I have identified cyber-activists as individuals (a) who aim to raise awareness on a particular issue of interest (b) through the publication of content on the Internet—whether it is music, art, blog posts, or news articles. For example, on November 8, 2015, Egyptian journalist Hossam Bahgat was detained and interrogated after writing and publishing online a report describing criminal convictions against 26 military officers for plotting a coup. He was charged with publishing false news "harmful to national security," a crime that can be punished with a jail sentence under the new counterterrorism law passed in July 2015. For the purposes of this research, Bahgat is considered to be a "cyber-activist."

Country selection

Below are the criteria I used in assessing whether or not to include the country in my research:

1. **Does the country have a counterterrorism law? If so, is the law published online or readily available otherwise (e.g., via contacts in the region)?**

   Much of this project involved tracking down legislation in its original language (Arabic) as well as accurately translated versions, if available. Most countries in the Arab world do not publish legal documents online, making the establishment of appropriate contacts crucial.

2. **If the country does not have a counterterrorism law, did the country's government and/or parliament debate a draft law?**

   This is important to keep in mind in following the debate on the balance between maintaining national security and protecting human rights online. Note, however, that the countries selected for study have a counterterrorism law in effect already.

3. How frequently do international media report on human rights violations in the country?

The third question was an assessment of how often human rights violations in the country featured in the international media. For example, Egypt is much more widely covered than Oman or Algeria.

Question 1 and Question 2 were asked in regard to cybercrime laws as well.

After conducting a topical study of the socio-political conditions of each Arab country, I started to pose the questions mentioned above and, based on the responses, I selected the following countries: Egypt, Jordan, Saudi Arabia, and Tunisia.

IV. Common threads

Commonality of a distinctive two-step process throughout the region

In studying the behavior of law enforcement authorities throughout the MENA region when targeting human rights advocates or political dissidents, a common pattern emerged. Authorities appeared to use a two-step process to effectively target human rights defenders or political dissidents. These two steps are outlined below.

Characterization of activity in question

The first step in stifling the individual's expression is for law enforcement to categorize the individual's activity. For example, Internet User A might use Facebook to write and publish posts criticizing her government. Her writing and publication could be considered journalism or, alternatively, speech. This initial characterization then leads to the type of law under which a police officer might decide to arrest the individual.

Determination of legal strategy for prosecution

Following the characterization of the activity, a law enforcement officer typically chooses one to two laws under which to arrest the individual. The public prosecutor and, in some cases, law enforcement officers themselves develop a legal strategy to best ensure the individual's successful conviction. In some cases, a judge may add subsequent charges during the trial. Using the example above, if Internet User A's activity is considered to be journalism, she will likely be tried under the country's publication code. If considered speech (which often has fewer protections than journalism), then it can be tried under another law—including cybercrime and counterterrorism. Further, an individual's activity may have more than one characterization. It can be said, then, that in most cases, there is a rule by law as opposed to a rule of law: the goal is to arrest, try, and punish the individual and the law is merely a tool used to reach an already predetermined conviction.

V. Cybercrime and counterterrorism: an ideal approach to criminalize non-violent action

Abuse of laws

In most countries, the promulgation of counterterrorism laws and regulations is typically executed with the intention of fighting violent, ideologically motivated crime while abiding by international human rights standards.[6] While governments and courts worldwide have struggled to articulate an exact definition of "terrorism," it is generally understood as violent fundamentalist activity of a greater magnitude and reach than typical crime. In the Arab world, one might expect such laws to be specifically tailored for the purpose of countering violent action by the likes of Al-Qaeda or ISIS.

Similarly, cybercrime laws are more often drafted to fight technical crimes that usually deal with issues of e-commerce and intellectual property—such as hacking into computers, theft of copyrighted material, and financial fraud. This is not so in the Arab world. Even if cybercrime laws criminalize such activities, there is little evidence that prosecutors have used them for this purpose.

> "Tunisia's draft cybercrime law, leaked on July 23, 2014, is full of ill-defined and vague provisions that allow law enforcement authorities to liberally stretch the meaning of clauses to extend to actions that are protected under international human rights standards."

The inefficiencies of counterterrorism laws are well studied in countries like the United States and the United Kingdom.[7] For example, in the United States, positive feedback loops in counterterrorism policies produce confirmation bias, leading law enforcement parties to target innocent suspects from racially and religiously marginalized groups.[8] This results in unjust prosecutions—mostly through pretextual charges and pseudo-entrapment.[9] In the Arab world, counterterrorism and cybercrime laws directly target political dissenters. The

6 *See*, 2005 World Summit Outcome (A/Res60/1), 24 October 2005: https://www.un.org/womenwatch/ods/A-RES-60-1-E.pdf.
7 Kent Roach, Sources and Trends in Post 9/11 Anti-Terrorism Laws (April 2006). U Toronto, Legal Studies Reasearch Paper No. 899291 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=899291.
8 *See,* Steven R. Morrison, The System of Domestic Counterterrorism Law Enforcement," Stanford Policy and Law Review, 341-374.
9 *Id.* at 370.

system of using both kinds of legislation rarely if ever produces positive results (capturing and/or halting criminal activity), and instead produces plenty of negative results—arresting individuals engaged in non-violent activity online that very frequently features critical attitudes towards the government. For example, Tunisia's draft cybercrime law, leaked on July 23, 2014, is full of ill-defined and vague provisions that allow law enforcement authorities to liberally stretch the meaning of clauses to extend to actions that are protected under international human rights standards—such as the right to privacy and free speech. Article 24 in the draft cybercrime law provides a six-month imprisonment and a fine of 5,000 Tunisian dinars (about USD 2,900) to anyone who uses "information and communications systems to spread content showing obscene acts and assaulting good morals." Punishment increases to a three-year jail sentence if the content in question "incites to immorality."[10] Such legalized punitive frameworks jeopardize the safety and free expression rights of all Internet users.

Vagueness and breadth of laws

In researching the laws of the four countries under study, one trend emerged clearly: whether the country actually uses the cybercrime or counterterrorism law as its primary means of targeting its citizens or not, the laws that do exist are consistently broad and vague. For example, Saudi Arabia's counterterrorism legislation criminalizes everything from "defaming the state" to "calling for atheist thought" (Law for Crimes of Terrorism and Financing, 2013). The law is so incredibly vague that it is difficult to conceive of an action that could not be prosecuted under its mandate. Generally, the more broadly drafted a law is, the more likely law enforcement will use it to target whomever they deem a threat the incumbent government.

10 *See*, "Leaked Cybercrime Law Could Undo Tunisia's Pioneer Status on Internet Rights," Afef Abrougi, 28 July 2014, https://advox.globalvoices.org/2014/07/29/leaked-cybercrime-law-could-undo-tunisias-pioneer-status-on-Internet-rights/.

VI. Analysis of each country's most commonly used legal reference

Egypt

Background

A country of 83 million people, Egypt is a key center of influence in the Arab world. Egypt continues to suffer through troubling times following the deposition of dictator Hosni Mubarak. The current political ecosystem in Egypt is fragile, and authorities have taken to using old methods of repression to stop critical speech.

The atmosphere has become even more polarized since the 2013 coup, when the Supreme Council of the Armed Forces (SCAF) deposed the elected president, Mohamed Morsi—Egypt's first elected civilian president and a high-ranking member of the Muslim Brotherhood—after demonstrations calling for early presidential elections. Egypt has been under military rule ever since. The human rights situation generally, and the Internet rights ecosystem specifically, is increasingly under attack.

The Egyptian parliament passed a counterterrorism law[11] in August 2015. The law is widely publicized and available online. I have accessed the text of the law through the Arab Digital Rights Dataset, which also provides an English translation. Egypt does not currently have a cybercrime law.

Protest law

My initial hypothesis about Egypt was that as soon as the parliament passed the counterterrorism law, the government would quickly begin using it as a bogus charge to target and arrest individuals on the basis on expression online.

After researching many cases of arrest, I learned that my hypothesis was incorrect. Of the hundreds of Internet-related arrests in Egypt, I was only able to document 28 cases with counterterrorism-related charges since 2012. Instead, the government relies primarily on an anti-protest law to stifle online speech.

11 Egypt Anti-Terrorism Law, http://smex.silk.co/page/Anti-terrorism-law.

On November 24, 2013, the government banned unlicensed street demonstrations.[12] This ban is now the most commonly used legal framework to criminalize online speech by activists.

"On November 24, 2013, the government banned unlicensed street demonstrations. This ban is now the most commonly used legal framework to criminalize online speech by activists."

For example, until September 30, 2015, at least 62 journalists have been detained or jailed for expressing themselves. Most of these journalists used the Internet to disseminate information and opinions, and most were arrested under precarious penal code charges.[13] 55 of those 62 have been detained after the start of 2014, indicating a sharp increase of arrests in the last two years. Imprisoning individuals on the basis of posts made on the Internet is a relatively new phenomenon in the country.

The best example is the closely followed case of Alaa Abdel Fattah—an internationally renowned software guru, blogger, and peaceful political activist. Only four days after the parliament passed the anti-protest law, on November 28, 2013, security forces raided Abdel Fattah's home. The officers beat him and his wife when asked to see their warrant and took and held him overnight, blindfolded and handcuffed, in an unknown location.

On December 9, 2013, the Public Prosecutor referred Abdel Fattah's case—along with three other defendants[14]—to a criminal court on the charge of "participating with unknown others in a gathering of more than 5 people, which might endanger public peace with the aim of committing crimes of assault on persons, public and private property and impeding the work of public authority using force and violence" under the penal code and the anti-protest law. They were sentenced to three years of hard labor and high fines.[15]

Abdel Fattah was initially detained for four months (from November 28, 2013 until provisional release on March 23, 2014). He was then re-arrested on June 11, 2014 and only released again on bail on September 16, 2014. On October 27, 2014, Abdel Fattah was detained again.

12 New York Times, "New Law in Egypt Effectively Bans Street Protests," 25 November 2013, http://www.nytimes.com/2013/11/26/world/middleeast/egypt-law-street-protests.html.
13 The Arabic Network for Human Rights Information, "Names of Egyptian Journalists in Prison Until Now," 30 September 2015, http://anhri.net/?p=151666&lang=en.
14 Ahmed Maher, Mohamed Adel, and Ahmed Douma, all founding members of the April 6 Movement and vocal human rights defenders in the country.
15 "Egypt Jails Ahmed Maher and Other Secular Activists," BBC, 22 December 2013, http://www.bbc.com/news/world-middle-east-25484064.

Abdel Fattah was sentenced in absentia during the month of June 2014 to 15 years of "rigorous imprisonment," but was arrested after the sentence. On February 23, 2015 a re-trial sentenced him to five years of rigorous imprisonment. Currently, he is held at Tora Prison —Egypt's notorious maximum-security detention center, historically used to hold men suspected of violent crimes and terrorism.

Alaa Abdel Fattah has the distinction of having been jailed or charged under every government to take power in Egypt in the last decade. In 2006, when he was only 22, he was jailed by the Mubarak regime. The Supreme Council of the Armed Forces (SCAF) jailed him in 2011 and Morsi brought a case against him in 2013. He is now imprisoned by SCAF, once again.

Egypt's use of the anti-protest law to target activists is very widespread. Authorities rarely use the counterterrorism law—it is newer, and pursuing a case under the law is likely to present some challenging legal complications. One notable exception is the case of Hossam Bahgat, a journalist with Mada Masr. Bahgat wrote a report describing criminal convictions against 26 military officers for plotting a coup. He was subsequently detained and interrogated on November 8, 2015.[16] He was charged with publishing false news "harmful to national security" under the new counterterrorism law.[17]

16 Amnesty International, "Egypt: Arrest of Prominent Activist Hossam Bahgat Another Blow for Freedom of Expression", 8 November 2015, https://www.amnesty.org/en/latest/news/2015/11/egypt-arrest-of-prominent-activist-hossam-bahgat-another-blow-for-freedom-of-expression/.

17 Jadaliyya, "Rights Groups Outraged by Hossam Bahgat's Detention, Demand His Immediate Release," 10 November 2015, http://www.jadaliyya.com/pages/index/23152/rights-groups-outraged-by-hossam-bahgat%E2%80%99s-detention.

Hossam Bahgat (Egypt)

Journalist, activist

Charged under Egyptian counterterrorism law of 2015

Hossam Bahgat is a leading investigative journalist who mostly writes for the news website Mada Masr. He is also the founder of the Egyptian Initiative for Personal Rights (EIPR), a highly respected human rights advocacy group. On October 13, 2015, Bahgat wrote a report investigating the criminal convictions of 26 military officers for plotting a coup. Following the publication of his article online, Bahgat was subsequently detained and interrogated on November 7, 2015. He was kept in a small, dark cell with nothing but two blankets on the floor. Bahgat was charged with publishing false news "harmful to national security" – a crime that can be punished with a jail sentence of up to three years under the new counterterrorism law passed in July 2015. Bahgat was released three days after his arrest on November 10.

Another more extreme case of state-sponsored infringements on freedom of expression and privacy online is the Egyptian government's push to prosecute LGBTQ-identified citizens through using online social media platforms. Though homosexuality is not illegal in Egypt, police have been using social media and smartphone applications (such as gay dating application Grindr) to hunt down and arrest gays and lesbians. Egyptian LGBTQ rights activists have published numerous messages warning members of the community to refrain from using these applications.[18] According to activists, at least 77 LGBTQ-identified people have been arrested since October 2013,[19] whose arrests were facilitated by the Internet.

Jordan

Background

Bordering both Iraq and Syria, Jordan's security concerns are not unfounded. The growth of the so-called Islamic State organization (ISIS) in Syria and Iraq is testing the kingdom's ability to protect its territory while respecting its international human rights obligations.

Following ISIS's capture and execution of Jordanian pilot Lieutenant Moath al Kasasbeh in Syria in early 2015, King Abdullah II vowed to wage a "relentless" war against ISIS and "hit them in their own ground."[20] But rather than attempting to thwart terrorist activity,

18 "Egyptian police use dating sites to hunt down gay people," France24, 16 September 2014, http://observers.france24.com/content/20140916-egyptian-police-dating-sites-gay.
19 *See*, http://76crimes.com/2014/05/19/crackdown-in-lgbt-egyptians-77-arrests-sinceoctober/.
20 Ian Black, "Jordan's King Abdullah Vows 'Relentless' War Against Isis," The Guardian, 4 February 2015, http://www.theguardian.com/world/2015/feb/04/jordan-king-abdullah-war-isis-pilot.

Jordan's internal security services are increasingly punishing innocent human rights defenders and government critics.

The Jordanian government's practice of silencing critical voices is not novel. For instance, on September 17, 2013, police arrested Nidhal al-Fara'nah and Amjad Mu'ala—publisher and editor of the Jafra News website, respectively—after it posted a third-party YouTube video that authorities deemed insulting to the brother of Qatar's ruler. Prosecutors charged both men with "disturbing relations with a foreign state" before the State Security Court, a court that has traditionally tried terrorism cases and whose judges include military officers.[21] Jordan has prominent and well-publicized cybercrime laws that are often cited by national courts. The cybercrime law was passed as the "Information Systems Crimes Law" in 2010 and is arguably the most developed cybercrime law in the region. Jordan also has a counterterrorism law that initially passed in 2006 but was significantly amended in 2014. I have accessed the text of both the cybercrime and counterterrorism laws through the Arab Digital Rights Dataset.

In addition to the counterterrorism law, the Jordanian penal code classifies other vaguely worded offenses (such as "undermining the political regime") as terrorism. The State Security Court has jurisdiction over these offenses as well, and will still be able to try peaceful protesters and others that are charged with them. In January 2014, the government amended the State Security Court law to restrict the court's jurisdiction to terrorism, espionage, treason, money counterfeiting, and drug offenses.

Cybercrime law, counterterrorism law

In June 2014, Jordan issued amendments to its 2006 Anti-Terrorism Law that broaden the definition of terrorism to include provisions that threaten freedom of expression. The original definition in the 2006 law read as follows: "any intentional act committed by any means that leads to the death of a person or causes bodily harm or damaging public or private property ... with the goal of harming public order and subjecting the peace of society or its security to danger."[22] Today, the 2014 amendments to this definition include acts such as "disturbing [Jordan's] relations with a foreign state," a charge already criminalized in the penal code that is regularly used to punish peaceful criticism of foreign countries or their rulers. The amendments remove the requirement that the action be connected to an act of violence, instead vaguely referencing acts that "sow discord" or "disturb public order." According to the 2014 amendments, the following acts are now considered terrorism:

21 World Report 2014: Jordan, Human Rights Watch, https://www.hrw.org/world-report/2014/country-chapters/jordan.
22 "Jordan: Terrorism Amendments Threaten Rights, Greatly Expand Categories of Terrorist Acts," Human Rights Watch, 17 May 2014, https://www.hrw.org/news/2014/05/17/jordan-terrorism-amendments-threaten-rights.

- Acts that subject the kingdom to danger of hostile acts, disturb its relations with a foreign state, or expose Jordanians to danger of acts of revenge against them or their money (Article 3(a));
- Any information system or network that facilitates terrorist acts, supports or spreads ideas of a group that undertakes an act of terrorism, or subjects Jordanians or their property to danger of hostile acts or acts of revenge (Article 3(e));
- Attacking the king or his freedom, the queen, the crown prince, or a guardian of the throne (Article 3(g));
- Any act committed with the intent to provoke an armed rebellion or changing the constitution in an unlawful way (Article 3(h)).

Vague provisions in the Jordanian counter-terrorism law make virtually any Jordanian citizen a suspect, and can easily extend to four million Jordanians currently online.[23]

Jamal Ayoub (Jordan)

Opinion and editorial writer

Charged under the 2014 amendments to Jordan's counterterrorism law of 2006

On April 23, 2015, opinion writer Jamal Ayoub was arrested after multiple news websites published an opinion piece he wrote that criticized Operation Decisive Storm, the bombing campaign by a Saudi-led coalition (that includes Jordan) against Houthi forces in Yemen. Jordan's State Security Court ordered Ayoub to be held for 15 days in Jordan's Marka prison, pending investigation into accusations that he disrupted the kingdom's relationships with foreign states. This action is punishable under the newly broadened anti-terrorism law, which the Jordanian parliament amended to include non-violent actions. Ayoub was released on August 17, 2015 – four months after his initial arrest.

The 2010 cybercrime law contains equally troubling provisions. The law bans abusive and provocative remarks that are made against a religion or promote hatred and threaten coexistence in the kingdom.[24] Article 10 criminalizes the use of information networks for the facilitation of terrorist activities with a sentence of hard labor: "Anyone who uses an information system or network to set up a website to facilitate terrorist activities or to support a group, organization or association which conducts terrorist activities, promotes its ideologies or finances shall be punished by temporary penal servitude." Article 11 further

23 "Jordan's Anti-Terrorism Law: A Choice Between Security and Speech," 7iber, 30 April 2014, http://7iber.com/2014/04/anti-terrorism-draft-law-a-choice-between-security-or-speech/.
24 Jordan, Information Systems Crimes Law, Article 11(a) and Article 11 (b).

criminalizes any end user accessing any website "that touches upon national security, foreign relations of the Kingdom, general security, or national economy" with a minimum of 4 months in prison.[25]

> "In Jordan, I found a total of 18 arrests for online activity related to counterterrorism, 8 of which occurred in 2015 alone; and a total of 4 cybercrime cases, 2 of which occurred in 2015."

My hypothesis about Jordan—that it uses counterterror and cybercrime as pretenses to arrest rights defenders—was proven right: authorities have not shied away from using these laws for this purpose. I found a total of 18 arrests for online activity related to counterterrorism, 8 of which occurred in 2015 alone; and a total of 4 cybercrime cases, 2 of which occurred in 2015. For example, Osama al-Ramini was arrested and held in detention in the Salt Prison for two weeks for publishing an article on his news website that was deemed "non-objective and full of slander" by authorities.[26] He was charged under the cybercrime law. A month later, on November 3, 2015, authorities arrested journalist Tareq Abu al-Ragheb for posting allegedly insulting comments on Facebook. He was charged with defamation under the cybercrime law and was held in detention for a week.[27]

The increase in arrests in 2015 is worrisome. It is also important to reiterate that this paper only references publicly accessible sources of information in researching cases—there are undoubtedly plenty of arrests and/or detentions that go undocumented and unreported.

Saudi Arabia

Background

Saudi Arabia represents a unique case in the Arab world because while there are plenty of cases of arrest reported via social media and some local news outlets, few national and international media platforms take note. The country remains largely understudied in the field of digital rights. Furthermore, online access to court documentation is very limited.

25 Jordan, Information Systems Crimes Law, Article 11(a): "Anyone who intentionally and without authorization or in violation or excess of an authorization accesses a website or information system in any manner with the purpose of viewing data or information that is not available to the public and which touches upon national security, foreign relations of the Kingdom, general security or national economy, shall be punished by imprisonment for a term not less than four months and by a fine not less than (500) five hundred dinars and not exceeding (5,000) five thousand dinars."
26 "Al Balad Website's Chief Editor Detained for Violating 'E-Crimes Law," The Jordan Times, 20 October 2015, http://www.jordantimes.com/news/local/al-balad-website%E2%80%99s-chief-editor-detained-violating-e-crimes-law%E2%80%99.
27 "In Jordan, TV Anchor Charged Under Cybercrime Law for Facebook Post," Committee for the Protection of Journalists, 6 November 2015, https://cpj.org/2015/11/in-jordan-tv-anchor-charged-under-cybercrimes-law-.php.

Saudi Arabia's promotion of the Internet as a tool for growth and economic prosperity has led the country to have one of the highest mobile penetration rates in the region.[28] Over 49 percent of Saudis have Internet access.[29] Saudis remain some of the most active social media users in the region, too, making the Internet a crucial public space that activists use to raise awareness—and like any public space in the country, authorities are keen on monitoring and suppressing speech. While critical voices find may find a home online, they are also heavily repressed.

For example, in October 2013, Saudi Arabian women took to the roads to protest the Saudi ban on women driving. The campaign, dubbed "Women2Drive," saw women driving in Saudi Arabia in defiance of the government ban and posting their videos on YouTube. Social media was key to spreading awareness, and word spread fast on Facebook and Twitter. The government responded by blocking the campaign's website, just after it collected over 11,000 signatures of support in only a few days.

Many of the women who protested the driving ban were harassed both online and offline. Government trolls took to Twitter and other social media platforms to attack women who had posted videos of themselves driving. Ministry of Interior employees called each woman individually to tell her not to drive. The ministry also issued a statement saying that any social media used for "banned gatherings and marches" to encourage women to drive were illegal. The statement also threatened to use force against the women: "The Interior Ministry confirms to all that the concerned authorities will enforce the law against all the violators with firmness and force."[30]

Saudi Arabia has several legal instruments criminalizing behavior that it deems terrorist activity. On January 31, 2014, Saudi authorities promulgated the "Penal Law for Crimes of Terrorism and its Financing." On March 7, 2014, the Interior Ministry issued further regulations designating an initial list of groups the government considers terrorist organizations, and further articulating activities that are punishable as 'terrorism."[31]

Saudi Arabia approved a cybercrime law on March 26, 2007. I have accessed both the counterterrorism and cybercrime laws through the Arab Digital Rights Dataset. Both laws have garnered the attention of international nonprofits such as Human Rights Watch, Amnesty International, and the Gulf Center for Human Rights. However, as is the case in most other Arab countries, we can only guess at the exact number of people that are prosecuted under them.

---

28 http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf.
29 "Challenging the Red Lines: Stories of Rights Activists in Saudi Arabia," Human Rights Watch, 17 December 2013, https://www.hrw.org/report/2013/12/17/challenging-red-lines/stories-rights-activists-saudi-arabia.
30 "Saudi Government to "Use Force" Against Women Protesting Driving Ban," UN Watch, 24 October 2013, https://www.kintera.org/cms.asp?id=4741612&campaign_id=65378.
31 Ministry of the Interior statement on "security and intellectual prohibitions on citizens and residents," 7 March 2014, http://www.spa.gov.sa/viewstory.php?newsid=1206710.

> "As is the case in most other Arab countries, we can only know the tip of the iceberg as to the exact number of people that are prosecuted under counterterrorism and cybercrime laws."

Counterterrorism law

Throughout 2013, 2014, and 2015, Saudi Arabia continued to arrest, try, and convict human rights defenders and outspoken critics. Courts rely heavily on the counterterrorism law to judicially harass Internet users. Saudi Arabia's counterterrorism laws are almost explicitly made for the very purpose of silencing peaceful dissent. The law criminalizes virtually all dissident thought or expression as terrorism. The 2014 law differs significantly from a 2011 draft, most notably by removing all sentencing guidelines, removing a blanket ban on participation in demonstrations, and removing provisions criminalizing as defamation statements calling the King or the state an unbeliever.[32] The Specialized Criminal Court, established in 2008, is mandated to try terrorism cases—which, much of the time, are human rights cases.

While purportedly combatting terrorism and disrupting extremist communications, authorities have instead taken to directly targeting and jailing online activists. Global nonprofits have documented this type of targeting—Freedom House's Freedom on the Net reports have documented Saudi Arabia's use of cybercrime and counterterrorism legislation for repressing liberal and critical commentary online for years.[33] The use of these laws has very real consequences for critics of the government.

From 2011 until today, at least 39 individuals have been jailed under the pretense of counterterrorism for expressing themselves online. Many of these individuals have been in and out of jail several times—for composing a tweet, liking a Facebook post, or writing a blog post.

32 "Saudi Arabia: Terrorism Law Tramples on Rights, Establishes Legal Veneer for Unlawful Practices," Human Rights Watch, 6 February 2014, https://www.hrw.org/news/2014/02/06/saudi-arabia-terrorism-law-tramples-rights.
33 Saudi Arabia: Freedom on the Net (2015), Freedom House, https://freedomhouse.org/report/freedom-net/2015/saudi-arabia.

Waleed Abu Al-Khair (Saudi Arabia)

Lawyer, activist

Charged under the Saudi Arabian ant-cybercrime law of 2007

Waleed Abu Al-Khair is a human rights lawyer and the founder of the Saudi Monitor of Human Rights. He has previously represented Raif Badawi, another prisoner of conscience from Saudi Arabia, and was very active on social media in advocating for human rights reform.

Abu Al-Khair was charged on May 28, 2014 under the anti-cybercrime law for allegedly preparing, storing and sending information that prejudices public order. He was also found guilty of "inflaming public opinion", "insulting the judiciary", "harming public order", and founding an unlicensed organization.

On July 6, he was sentenced to 15 years in prison (five years of which were suspended) and ordered to pay a 200,000 SR fine (about 53,000 USD). He was also ordered to disband his organization. On January 12, 2015, the Specialized Criminal Court in the Riyadh removed the five-year suspended jail term, and sentenced him to a full 15 years in prison. The jurisdiction of the Specialized Criminal Court is to deal with terrorism related cases, but it is increasingly being used to target human rights defenders. Abu Al-Khair is currently is still serving his sentence.

Under Saudi Arabian law, arresting individuals for even the most minor opposition to the government is perfectly legal. For instance, sweeping regulations published in the March 7, 2014, statement released by the Saudi Arabian Ministry of the Interior punishes virtually any non-violent and peaceful expression. The law's "terrorism" provisions criminalize the following activities:

- "Calling for atheist thought in any manner, or calling into question the fundamentals of Islam upon which this country is based," (Article 1);
- "Anyone who strips away their loyalty to the country's rulers, or who swears allegiance to any party, organization, ideology, group, or individual inside or outside [the kingdom]," (Article 2);
- "Anyone who aids terrorist organizations, groups, ideologies, associations, or parties, or demonstrates affiliation with them, or sympathy with them, or promotes them, or holds meetings under their umbrella, either inside or outside the kingdom; this includes participation in audio, written, or visual media; social media in its audio, written, or visual forms; Internet websites; or circulating their contents in any form, or using slogans of these groups and currents [of thought], or any symbols which point to support or sympathy with them," (Article 4);
- "Contact or correspondence with any groups, currents [of thought], or individuals hostile to the kingdom," (Article 6);
- "Seeking to shake the social fabric or national cohesion, or calling, participating,

promoting, or inciting sit-ins, protests, meetings, or group statements in any form, or anyone who harms the unity or stability of the kingdom by any means," (Article 8);

- "Attending conferences, seminars, or meetings inside or outside [the Kingdom] that target the security of society, or sowing discord in society," (Article 9); and
- "Inciting or making countries, committees, or international organizations antagonistic to the kingdom." (Article 11).

Such sweeping language provides ample room for prosecutors to prosecute and convict peaceful individuals expressing themselves on the Internet. If the accused individuals are tried at all, their trials are held in secret in the Specialized Criminal Court. This is hardly surprising. Court proceedings in Saudi Arabia fall far short of international standards for fair trial[34] given that it routinely denies defendants the most basic fair trial guarantees, including the right to a lawyer, and passes sentences in closed proceedings.

Tunisia

Background

Following the latest elections in October 2014, Tunisia is experiencing a set of circumstances unprecedented in the Arab world. The country is undergoing a democratic transition and institutional reform following the ousting of former dictator Zine El-Abidine Ben Ali in 2011. Despite holding two peaceful elections and passing a constitution that is widely heralded as one of the most progressive in the Arab world,[35] the government continues to crack down on online activists. Notably, most arrests and detentions seem to go unchecked by the judiciary due to the government's claim to "legitimacy" through elections. The human rights situation is dire—and the government has grown increasingly creative in the types of legislation used to target human rights activism.

On November 6, 2013, the government announced by decree[36] the creation of the Technical Telecommunications Agency (ATT).[37] The agency was ostensibly created to fight the threat of cybercrime and cyber-terrorism, and is explicitly mandated to "exploit national monitoring systems of telecommunication traffic" for the purpose of "providing technical

34 Amnesty International, "Saudi Arabia" in Annual Report 2012, 2012, www.amnesty.org/en/region/saudi-arabia/report-2012#ai-reports.

35 *See,* Duncan Pickard, "Implementing Tunisia's New Constitution," Rafik Hariri Center for the Middle East, Atlantic Council, http://www.iemed.org/actualitat-en/noticies/publicacions/historic-de-publicacions/anuari-de-la-mediterrania/sumaris/avancaments-anuari-2013/Implementing%20Tunisias_Med%202014_00%20Med.%20en%20cifrasgraf.pdf.

36 "Décret n° 2013-4506 du 6 novembre 2013, relatif à la création de l'agence technique des télécommunications et fixant son organisation administrative, financière et les modalités de son fonctionnement," http://igmena.org/userfiles/files/Decree-No-2013-4506.pdf.

37 Al Huffington Post Maghreb, "Création de l'ATT 'Lutter contre la cybercriminalité' pour le ministère des TIC: 'Espionner les citoyens' pour le parti Pirate." 20 November 2013, http://www.huffpostmaghreb.com/2013/11/20/agence-telecommunication-_n_4310497.html.

support to the judicial investigations into the information systems of crimes and communication." The agency is considered by some to be illegal and unconstitutional[38], and rights activists call the ATT the "Tunisian NSA."[39]

Terrorist attacks in March 2014 and June 2014 added weight to the government's "anti-terrorism" efforts. In June 2015, the government created a special unit within the Ministry of the Interior called "Brigade 5." The unit is composed of 30 information security engineers, mandated under the counterterrorism law to track "cybercrimes" and "cyber-terrorism."[40] Most recently, on March 22, 2016, Prime Minister Habib Essid announced the creation of a permanent joint commission for the "fight against terrorism." Essid said that this entity will "reinforce the position of the state in the fight against terrorism and the threats to the democratic transition." Although it is purportedly mandated to raise awareness of the dangers of terrorism, the commission's composition reveals a less noble goal. Notably, the Commission unites experts from the intelligence, security and defense agencies, the telecommunication agency, and an investigatory judge specializing in terror cases––who is nominated by decree.[41] Events are unfolding in Tunisia at a rapid pace, making it imperative to study today.

Tunisia passed a sweeping and controversial counterterrorism law on July 25, 2015, replacing an older law from 2003. The law includes several ICT provisions and presents interception of communications and surveillance as a mechanism to gather evidence in ongoing criminal investigations.[42] The bill also creates a unit of judges specialized in terrorism cases[43] and hands investigations to the criminal investigation department of Tunis rather than units at the governorate level.[44] The Tunisian parliament proposed a cybercrime law that was leaked to the public on July 23, 2014, with equally vague and sweeping language. It has yet to pass. I have accessed both documents through the Arab Digital Rights Dataset.

38 "State of Surveillance: Tunisia," Privacy International, 2 March 2016, https://privacyinternational.org/node/743; Kais Berrjab, "Le décret n°4506-2013 relatif à la création de l'Agence Technique des Télécommunications (ATT): un raté de trop," 20 January 2014, http://ostez.blogspot.com/2014/01/le-decret-n4506-2013-relatif-latt-un.html.
39 Afef Abrougi, "Will Tunisia's ATT Ring in a New Era of Mass Surveillance?" GlobalVoices AdVox, 26 November 2013, https://advox.globalvoices.org/2013/11/26/will-tunisias-att-ring-in-a-new-era-of-mass-surveillance/.
40 Special report on "24 Hours," El-Hiwar Ettounsi, https://www.youtube.com/watch?v=UQ5gfa5hghw&feature=youtu.be&t=15m31s.
41 Article 48 of the Tunisian Code of Criminal Procedure.
42 Dhouha Ben Youssef, "Terrorism and ICT: Keeping Alive Old Surveillance Practices in Tunisia," Nawaat, 01 September 2015, https://nawaat.org/portail/2015/09/01/terrorism-and-ict-keeping-alive-old-surveillance-practices-in-tunisia/.
43 Loi organique n° 2015-26 du 7 août 2015, relative à la lutte contre les infractions terroristes et la répression du blanchiment d'argent, Article 38.
44 *Id.* at Article 36.

Noureddine Mbarki (Tunisia)

Journalist, blogger

Charged under Tunisian counterterrorism law of 2003

Noureddine Mbarki is the chief editor of news website Akher Khabar online. Mbarki was charged with "complicity in terrorism" for publishing a photograph of Seifeddine Rezgui, the gunman of the June 26 attack in Sousse that killed 38 foreigners, emerging from a car before he began shooting. Notably, the police called Mbarki's newspaper's publisher 45 minutes after the photo was published and requested its removal for the sake of the ongoing police investigation. After consulting with Mbarki, the publisher immediately withdrew the photo. Still, an investigative judge of the First Instance Tribunal brought the charges against Mbarki three days after the photo was published. Mbarki was subsequently charged under the counterterrorism law, which can bring a 5-12 year prison term.

Tunisia's fragile Internet freedoms are slowly eroding through the use of old laws dating back to the Ben Ali era.[45] Contrary to what I had initially hypothesized, I have found that Tunisian authorities have only seldom used counterterrorism laws to stifle dissent. Of the 11 cases I tracked wherein authorities prosecuted individuals for expressing themselves online, only 2 of them were charged under the counterterrorism law (excluding 62 anonymous arrests from 2014 to 2016). Despite having passed controversial and sweeping counterterrorism regulations, law enforcement authorities continue to use defamation provisions in the penal code and Law 52-1992, otherwise known as the "anti-marijuana law." While my scope of research did not track defamation and drug-related cases, I offer some examples below to illustrate how these laws are used.

Defamation

In Tunisia, the best-publicized cases involving online activity have related to "defaming" the state or the military. For example, in April 2014, Rached Khiari, director of the Al Sada News website, received a three-month suspended sentence for defamation after publishing a video in which a third party insulted a judge. The specific defamation provision Khiari was prosecuted under comes from article 86 in the Telecommunications Code,[46] for "insulting others through public communication networks." Although he is the director of a news publication, Khiari was not prosecuted under the 2011 press code.[47] In the video, published

45 Tunisia: Freedom on the Net (2015), Freedom House, https://freedomhouse.org/report/freedom-net/2015/tunisia.
46 Business News, "Rached Khiari risque deux ans de prison," 22 April 2014, http://www.businessnews.com.tn/rached-khiari-risque-deux-ans-de-prison,520,45854,3.
47 Tunisia: Freedom on the Net (2015).

in March 2014, a mother cursed a judge who sentenced her son, a controversial Islamist activist, to jail. The mother received a three-month prison sentence. Khiari was initially faced with up to two years in prison for publishing the video. He was arrested again and held in detention for one day on January 4, 2016.

In another case, in December 2014, Tunisian authorities arrested prominent activist and blogger Yassine Ayari as he returned to Tunis from a trip abroad. His arrest came six weeks after he was sentenced in absentia to three years in prison by a military court for defaming the military institution. Ayari was sentenced under article 91 of the military justice code. [48] He was found guilty of "defaming army officers and senior defense ministry officials" in a series of Facebook posts in which he criticized Minister of Defense Ghazi Jeribi for refusing to appoint a new head of military intelligence and for weakening military institutions.[49] In a retrial held on January 20, Ayari's verdict was reduced to a one-year sentence.[50] Ayari appealed his conviction and on March 3, 2014 the military court of appeals reduced his jail term to six months.[51] Ayari was released on April 17.[52]

Officers also use a related penal provision that criminalizes "verbally insulting a public official while carrying out duties."[53] This specific provision has been used by the former Ben Ali government against members of the opposition, and is used today against protestors (especially those participating in sit-ins).[54] For example, film director Ines Ben Othmane was arrested on December 19, 2014, because of a Facebook status she posted complaining about months of harassment by the deputy head of the local police station. Because this post, she was sentenced to two months in prison for "insulting a public officer." She was later released on January 16, 2015.[55]

Anti-Drug Law

The fabrication of charges founded upon marijuana possession is a practice traditionally used by Tunisian authorities both before and after the uprisings to disguise politically

48 "Tunisia arrests blogger for defaming army officers," *Al Akhbar English*, 26 December 2014, http://bit.ly/1EFMdGs.
49 "Tunisia: Blogger Convicted by Military Court: 3 Years in Jail for Facebook Posts," Human Rights Watch, 6 January 2015, https://www.hrw.org/news/2015/01/06/tunisia-blogger-convicted-military-court.
50 "Tunisia: Blogger Sentenced to One Year in Jail for Criticizing Army," Amnesty International, 20 January 2015, https://www.amnesty.org/en/latest/news/2015/01/tunisia-blogger-sentenced-one-year-jail-criticizing-army/?linkId=11848922.
51 "Military Court Sentences Blogger to Six Months in Jail," Middle East Eye, 3 March 2015, https://www.amnesty.org/en/latest/news/2015/01/tunisia-blogger-sentenced-one-year-jail-criticizing-army/?linkId=11848922/.
52 "Blogger Yassine Ayari To Be Released Today," TunisiaLive, 16 April 2015, http://www.tunisia-live.net/2015/04/16/blogger-yassine-ayari-to-be-released-today/.
53 Tunisian Penal Code, Articles 125-130 § II.
54 Interview with Moutaa Amin Elwaer, member of the Manich Msameh Movement, 10 April 2016.
55 "Film Director Ines Ben Othman Released," 21 January 2015, Amnesty International, https://www.amnestyusa.org/get-involved/take-action-now/good-news-tunisia-film-director-ines-ben-othman-released-ua-315.

motivated arrests.[56] In November 2015 alone, the Ministry of the Interior arrested over 2,000 people, 516 of which were arrested for the alleged consumption of cannabis[57]—many of them were activists or prominent voices on privacy and security online. Before the terrorist attacks in 2014, there had been only 10 to 12 people arrested on the charge of cannabis consumption or possession.

> "In November 2015 alone, the Tunisian Ministry of the Interior arrested over 2,000 people—516 of which were arrested for the alleged consumption of cannabis."

Several other Tunisians have been detained or suffered legal harassment on vague defamation or anti-drug charges. They mostly remain anonymous.

Interior Ministry's Anonymous Arrests

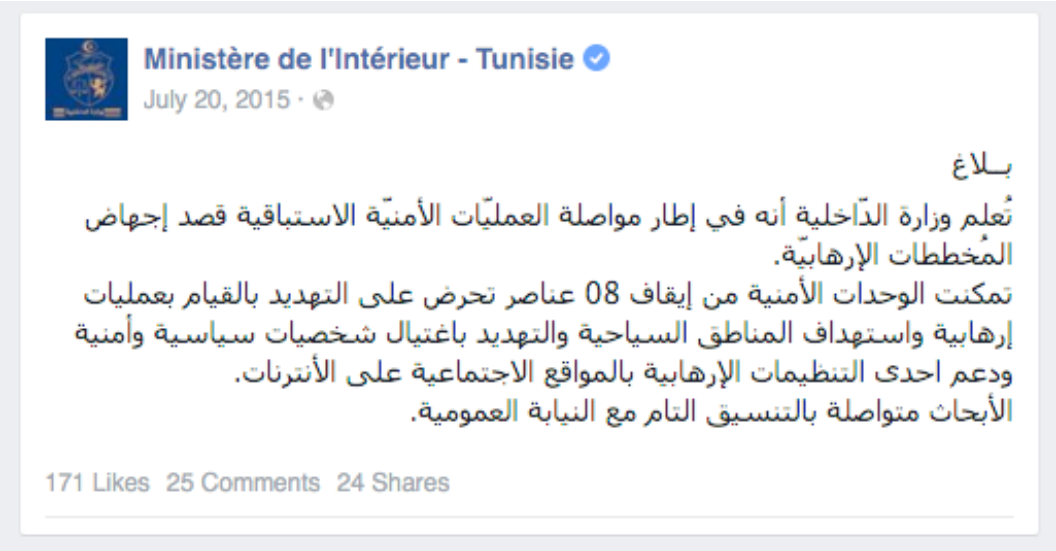
Despite the availability of counterterrorism laws, Tunisia's Ministry of the Interior continues to circumvent due process and arrest individuals anonymously.

What is notable in Tunisia is the Ministry of the Interior's common practice of issuing press releases announcing the arrest of "terrorists" because of their social media activity. The Ministry is very active on social media, particularly on Facebook. From 2011 to 2016, the Ministry has published over 8,200 posts. These posts are usually press releases highlighting what the Ministry has "accomplished" in terms of arrests and seizures. Of these releases, I have found a total of at least 12 instances wherein law enforcement authorities arrest individuals for their online activity. A total of 62 persons have been arrested for social media activity, usually on Facebook or Twitter. Their arrests usually evade proper legal procedure.

> "The Ministry of the Interior has arrested a total of 62 anonymous persons for social media activity, usually on Facebook or Twitter. Their arrests evade proper legal procedure. The Ministry usually keeps the identities of those arrested anonymous, labeling them instead as 'terrorists.'"

56 Global Voices Advocacy, "Tunisian Activist Azyz Amami Arrested on Drug Charges," 13 May 2014, https://advox.globalvoices.org/2014/05/14/tunisian-activist-azyz-amami-arrested-on-drug-charges/.
57 Official figure released by the Tunisian Ministry of the Interior, 5 December 2015, https://www.facebook.com/ministere.interieur.tunisie/posts/1157245544302820.

Below is an example of a press release on Facebook announcing this type of arrest:



"Announcement: The Ministry of Interior has managed to arrest 8 individuals that are inciting the following activities: carrying out terrorist attacks targeting touristic areas, the assassination of security and political figures, and supporting a terrorist organization via social media on the Internet. In collaboration with the public prosecutor, the investigation continues."

The Ministry usually keeps the identities of those arrested anonymous, labeling them instead as "terrorists." Not only are we unable to know which exact authority arrested these individuals, we also do not know under which law or mandate they are acting under. There is usually little indication of the laws the individuals are charged with breaking, or their whereabouts following the arrest.

In reviewing the Ministry's posts regarding the arrest and/or capture of individuals for online activity under the guise of terrorism, it is alarming how little resistance the Ministry faces in its arrests. It has the unimpeded ability to monitor Internet activity and all political, religious, and advocacy groups without any evidence of wrongdoing.

VII. Diversity of framework: there is no "MENA"

Political context heavily influences method of criminalization

More than anything else, this research demonstrates that the regional approach to addressing issues of Internet freedom in the so-called "MENA" region is dead. Each country has a different socio-political context and institutional history that influences which laws suit the goals of the repressive government in question.

Diminishing territorial integrity

Furthermore, the spillover of the war in Syria has led to the territorial disintegration of several Arab countries such as Iraq and Syria. ISIS controls large swaths of land in both countries,[58] and within those areas, state institutions have been reduced to rubble. This means that in Iraq and Syria, information flows and controls are no longer under the jurisdiction of the state—requiring an entirely new lens through which to research the question of politically motivated arrests of online activists.

> "It is important to connect a government's actions online to the changing political situation on the ground."

It is important to connect a government's actions online to the changing political situation on the ground. In Tunisia, for example, the government is struggling to keep its disillusioned youth from traveling to Syria to fight with IS, who make up the majority of foreign recruits.[59] Like combatting terrorism, such a policy goal often lends itself to the blind arrest of Internet users without granting them due process—furthering the severe abuse of basic political rights and civil liberties.

58 "Islamic State Group: Crisis in Seven Charts," BBC, 30 March 2016, http://www.bbc.com/news/world-middle-east-27838034.
59 *Id.*

VIII. Conclusion

Contextualization today entirely different from 2011

In each of the countries studied, politically motivated arrests of online activists are on the rise.

In Jordan, the highest number of arrests of Internet users under the counterterrorism law occurred in 2015. Mass arrests in Egypt under the anti-protest law have become the norm—if not already imprisoned, thousands of youth who used the Internet as a primary means of organizing[60] have been arbitrarily arrested and detained.[61] In Tunisia, the old guard—mostly the "political police" that works in the Ministry of the Interior that has been instrumentalized to achieve political ends for decades[62]—continues to rely on certain clauses in the penal code such as defamation and anti-drug laws to harass and arrest online users. And finally, the Kingdom of Saudi Arabia continues to use its counterterrorism regulations —unchecked—to stop reform efforts before they even begin. As these governments continue to quell reform, one can safely assume that further restrictions on online activity and speech are on the way.

> "Protecting the homeland from terrorist threats has become the primary justification to shut down unwanted speech. But it is one thing to assert a conflict between security and liberty, and another to explicitly set aside the very possibility of freedom in the name of security."

The prosecution of bloggers and online activists represents only one angle of a greater strategy that these governments employ in limiting Internet use. All four countries studied in this report have a history of broad censorship, arbitrary monitoring and blocking of critical websites, and infiltration of opposition social media pages. While each country uses a

60 "Online Activism Fuels Egypt Protest," Aljazeera, 28 January 2011, http://www.aljazeera.com/news/middleeast/2011/01/201112810225384873O.html.
61 "Egypt: Generation of Young Activists Imprisoned in Ruthless Bid to Crush Dissent", Amnesty International, 30 June 2015, https://www.amnesty.org/en/latest/news/2015/06/egypt-generation-of-young-activists-imprisoned-in-ruthless-bid-to-crush-dissent/.
62 "State of Surveillance: Tunisia," Privacy International, 2 March 2016, https://privacyinternational.org/node/743.

different legal strategy to shut out dissent, all four of them do so under the pretext of national security. Protecting the homeland from terrorist threats has become the primary justification to shut down unwanted speech. Law enforcement in all four countries arrest vocal Internet advocates and send them to the judiciary, where, to varying degrees, the activists endure sham trials only to be locked up in prison. In my study on the judicial record of these laws, I did not find any examples of law enforcement arresting and detaining actual hackers attempting to break into critical infrastructure or otherwise engage in detrimental criminal activity online.

In each country studied, the threat of fundamentalist terrorist activity is undoubtedly legitimate. But it is one thing to assert a conflict between security and liberty, and another to explicitly set aside the very possibility of freedom in the name of security. The trend is clear: law enforcement consistently abuses laws to suit the needs of opportunistic politicians. It is driving critical voices to extinction by locking up those who dare speak up, and instilling self-censorship in those that remain free. By repressing peaceful public discourse, the state indirectly contributes to the fundamentalism it claims to fight.

When that happens, the state itself becomes the terrorist.